COMPAQ

T1500 WINDOWS-BASED TERMINAL NETWORK INSTALLATION GUIDE

COMPAQ

T1500 WINDOWS-BASED TERMINAL NETWORK INSTALLATION GUIDE

December 1999

Notice

The information in this document is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

Compaq T1500 Windows-based Terminal Reference Guide

First Edition December 1999

Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Compaq Computer Corporation may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Canadian Notice

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Avis Canadien

Cet appareil numérique de la classe B respecte toutes les exigneces du Réglement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards):

- EN55022 (CISPR 22) - Electromagnetic Interference
- EN50082-1 (IEC801-2, IEC801-3, IEC801-4) - Electromagnetic Immunity
- EN60950 (IEC950) - Product Safety

Japanese Notice

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

Control No. 075C

License Agreement

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS SOFTWARE (TOGETHER WITH ANY SUPPLIED DOCUMENTATION, HEREAFTER “SOFTWARE”), WHICH IS COPYRIGHTED BY LICENSOR. USING THIS SOFTWARE INDICATES YOUR ACCEPTANCE OF THE FOLLOWING TERMS AND CONDITIONS.

Grant

You may use the Software in conjunction with Your hardware (Terminal). You have the right to use this Software by loading it onto a computer containing the capability of transferring the Software (in whole or in part) to Your Terminal. You may use the Software in this fashion to as many times as is necessary, so long as such use is always in conjunction with Your Terminal. You may transfer ownership of the Terminal and equipment, including the right to use the Software to another party so long as that party agrees to accept these terms and conditions.

YOU MAY NOT USE, COPY, MODIFY, TRANSLATE OR TRANSFER THE SOFTWARE, OR MODIFICATION THEREOF, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE. YOU MAY NOT DECOMPILE, REVERSE ENGINEER OR OTHERWISE DECODE OR ALTER THE SOFTWARE.

Disclaimer of Warranty

The software is provided, “AS IS,” and is delivered with no warranties, either express or implied.

LICENSOR MAKES AND YOU RECEIVE NO WARRANTIES ON THE SOFTWARE, EXPRESS, IMPLIED, OR STATUTORY, OR IN ANY OTHER PROVISION OF THIS AGREEMENT OR COMMUNICATION WITH YOU, AND LICENSOR DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR ANY PARTICULAR PURPOSE. LICENSOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION WILL BE UNINTERRUPTED OR ERROR FREE.

SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

Limit of liability

UNDER NO CIRCUMSTANCES SHALL LICENSOR BE LIABLE FOR LOSS OF DATA, COST OF COVER, OR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THESE LIMITATIONS SHALL APPLY EVEN IF LICENSOR OR ITS RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

YOU AGREE THAT THESE ARE THE ONLY APPLICABLE TERMS OF AGREEMENT BETWEEN US COVERING SOFTWARE AND THAT THEY SUPERSEDE ANY OTHER COMMUNICATIONS (ORAL OR WRITTEN) BETWEEN US RELATING TO THE SOFTWARE.

Export Restrictions

You agree You will not export or transmit the Software to any country to which export is restricted by applicable U.S. law or regulation without the written approval of the appropriate U.S. Government organization.

U.S. Government Restricted Rights

The Software is provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technological Data and computer software clause at DFARS 252.227-7013 or in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 8 C.F.R. 52-227-19 as applicable.

Contents

Overview

Introduction *xi*
How to Use This Guide *xi*
References *xi*
- DHCP/BOOTP *xii*
- Time Server *xii*
- SNMP *xii*
- Other RFCs *xii*

1 Installation Overview and Planning

Overview of Installation Procedure *2*
Planning Your Installation *3*
- Step 1. Complete Worksheets *3*
- Step 2. Configure Terminal Start-Up Resources *3*
- Step 3. Configure Optional Terminal Start-Up Resources *4*
- Step 4. Configure Server Application Resources *4*
- Step 5. Select Location of Browser *4*
- Step 6. Install CD Software onto the Server(s) *4*

2 Configuring Terminal Start-Up Resources

BOOTP *5*
DHCP *8*
- T1500-Specific Option Definitions *13*

Option 43 Vendor-Specific ID *13*
NETSVC *13*
NOSWAP *14*
REFLASH *14*
MF_DIR *14*
MF_CFG *15*
XFS *15*
XDMCP *15*
BUDDY_BOOT *15*
Packet Size *16*
Option Overload *16*
Option 18 vs. Option 43 vs. Options 128+ *17*
Option 18 *17*
Option 43 *19*
Options 128+ *19*
TFTP *20*
NFS *20*
DNS *22*
Time Server *22*

3 Configuring Optional Terminal Start-Up Resources

Network Services *23*
NFS *24*
SMB *24*
SNMP *25*
HTTP (Help) *26*
Serial Internet Connections *26*
PPP *26*
SLIP *26*
CSLIP *27*
FTP *27*
HTTP (Upgrades) *27*

4 Configuring Server Application Resources

HTTP *29*
POP3/IMAP4 *30*
ICA *30*
RSH (X Manager) *30*
Secure Shell *32*

5 Selecting Browser Location

Browser Location *35*
Netscape Communicator Constraints *36*

6 Installing CD Software onto the Server(s)

CD Contents *39*
Running the Installation Program *39*
- Text-Mode Installation *43*
- GUI-Mode Installation *44*

Installing on Non-Supported Servers *45*

A T1500 Windows-Based Terminal Quick-Start Instructions

Quick-Start Procedure *48*
“G-Key Reset” Procedure *50*

B Installation Planning Worksheets

Terminal Start-Up Resources Worksheet *53*
Optional Terminal Start-up Resources Worksheet *54*
Server Application Resources Worksheet *55*
Browser Launch Location Resources Worksheet *56*
Other Images Location Worksheet *57*
Software Images from the CDROM Worksheet *58*

List of Figures

2-1 Bootptab File Example *7*

List of Tables

2-1 DHCP Options *10*
2-2 Additional Vendor-Specific Options *12*
2-3 Labels and Data for Text Format Option *17*
5-1 Netscape Communicator Constraints *37*

x

Overview

Introduction

This guide explains how to install software from the installation CD onto your server and how to configure the resources resident on the server to support Compaq T1500 Windows-Based Terminals for this software release.

How to Use This Guide

For full access to all the terminal resources, you will need to plan and configure your server setup as explained in Chapter 1 of this guide.

If you only want to verify basic operation of the terminal using local boot, go directly to the quick-start procedure in Appendix A. However, you will have only limited access to the terminal resources.

Terminal setup information is available from help files resident on the terminals and complete instructions are available on line after terminal-server communication is established.

References

The following Requests for Comments (RFCs) should be reviewed:

Note

RFCs are freely available through the World-Wide Web. They can be accessed from sites such as: *http://www.cis.ohio-state.edu/hypertext/information/rfc.html*

DHCP/BOOTP

RFC 1534 - Interoperation between DHCP and BOOTP

RFC 2131 - Dynamic Host Configuration Protocol

RFC 2132 - DHCP Options and BOOTP Vendor Extensions

Time Server

RFC 868 - Time Protocol

SNMP

RFC 1155 - Structure and Identification of Management Information for TCP/IP-based Internets

RFC 1157 - A Simple Network Management Protocol (SNMP)

RFC 1212 - Concise MIB Definitions

RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II

Other RFCs

RFC 1350 -The TFTP Protocol (Revision 2)

RFC 1094 - NFS: Network File System Protocol Specification

RFC 1034 - Domain Names - Concepts and Facilities

RFC 1035 - Domain Names - Implementation and Specification

RFC 2616 - Hypertext Transfer Protocol - HTTP/1.1

RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication

RFC 1548 - The Point-to-Point Protocol (PPP)

RFC 1055 - A Nonstandard for Transmission of IP Datagrams Over Serial Lines: SLIP

RFC 1939 - Post Office Protocol - Version 3

RFC 821 - Simple Mail Transfer Protocol

1 Installation Overview and Planning

This document describes how to install the T1500 software on the following computer servers:

- SCO OpenServer 5.0.5
- SCO UnixWare 7
- Linux (both Slackware and Red Hat)
- Windows NT Server
- HP/UX

For technical support refer to the Compaq Technical Support telephone numbers for your area.

Note

If you are operating in a local-boot environment and already have a network configured, and if you will be using the default help page and time server, you might consider using the quick-start procedure in Appendix A rather than this procedure. Otherwise, use this advanced procedure.

Note

If prior-release terminals are running on your network, be careful to avoid overwriting the prior-release files when installing this version of software.

Server resources can be provided from platforms other than the above-listed ones, but Compaq has not certified other environments and can not be responsible for any problems related to incorrectly configured servers. If you are going to operate in a different server environment, read this entire document very carefully to determine if there are any issues that you might need to resolve.

Overview of Installation Procedure

There are two major parts to the installation:

1. The first part is the configuration of the server resources necessary to use the terminal.
2. The second part is the installation of software provided on the installation CD.

The installation scripts on the CD are used to perform the second part; they are not used for the first part because software tools should already exist on your server to configure the server resources.

Note

Because portions of the software installed from the CD depend on certain server resources, it is recommended that you configure the server resources first before installing software from the CD.

This document provides all the steps necessary to configure a complete set of server resources for use with the terminals for this software release. For most of the resources, you should refer to the instructions and manual pages that come with the server software and operating system running on your server. Where special configuration information applies specifically to the terminals, this document provides that information. Many servers provide tools to configure the various network resources required, recommended, or requested for use with the terminals.

Planning Your Installation

The software installation procedure is broken down into 6 basic steps, including the planning described in this chapter. The following brief descriptions of the basic steps do not by themselves provide enough information for you to fill in the planning worksheets presented in Appendix B of this document; you should also read the chapters pertaining to the individual worksheets for full information. If you fill in the worksheets and perform the procedures presented in Chapters 2 through 6 in order, the installation should go smoothly.

Step 1. Complete Worksheets

The worksheets in Appendix B will help you determine which server resources must be installed/configured for the planned installation. Each worksheet pertains to one of the categories of network resources. Steps 2 through 6 below provide brief summaries of the configuration process, and Chapters 2 through 6 provide details pertaining to each corresponding step.

Note

Read the instructions presented in the chapter pertaining to a worksheet before filling in the worksheet. This will enable you to proceed smoothly through the remaining steps of this procedure.

Step 2. Configure Terminal Start-Up Resources

There is a minimum set of server resources that must be configured for using a T1500 Windows-Based Terminal. Some of the resources are required in a network-boot environment, some are required in a local boot environment, and others are strongly recommended for either environment.

Fill out the worksheet for Step 2 in Appendix B and use the instructions in Chapter 2 to configure terminal start-up resources.

Step 3. Configure Optional Terminal Start-Up Resources

A set of resources independent of the individual applications on the terminal is strongly recommended for ease of use of the system as a whole. Although these resources are optional, providing them will speed up access of certain items, provide enhanced diagnostic capabilities (for troubleshooting problems), provide for swapping in a local-boot environment, provide for print spooling in a local-boot environment, allow for remote administration of the terminal, provide for Internet (or intranet) connections via a modem, and facilitate upgrading the terminal to future revisions.

Fill out the worksheet for Step 3 in Appendix B and use the instructions in Chapter 3 to configure optional terminal start-up resources.

Step 4. Configure Server Application Resources

Some applications on the terminal require a server to be configured with services that the applications must access to operate properly.

Fill out the worksheet for Step 4 in Appendix B and use the instructions in Chapter 4 to configure server application resources.

Step 5. Select Location of Browser

A set of resources must be configured based on your choice of browser access. The choice should be based upon performance, features required, and administrative costs. The terminal is capable of running browsers locally, from a Windows Terminal Server (via the ICA protocol), and from a UNIX server (via the X protocol).

Fill out the worksheet for Step 5 in Appendix B and use the instructions in Chapter 5 to select the location of the browser.

Step 6. Install CD Software onto the Server(s)

After the server resources are configured, you must install software from the installation CD onto the server(s). You do not need to install all the software on the CD on all the servers. You need only to install the portions that correspond to server resources configured in steps 2 through 5 above, and they need to be installed on only the individual servers providing the associated server resources.

Fill out the worksheets for Step 6 in Appendix B and use the instructions in Chapter 6 to install CD software onto the server(s).

2 Configuring Terminal Start-Up Resources

Several network resources are either required or recommended for starting up the terminal initially in a network-boot environment. The resources in this category use the following 6 network protocols:

BOOTP	NFS	DHCP
DNS	TFTP	Time Server

A brief description of the resources and any special configuration requirements for each protocol are provided in this chapter. Some resources (such as NFS) may also be described in other chapters of this document.

BOOTP

BOOTP is a protocol used in a network-boot environment for providing all information that the terminal needs to start with minimal functionality. Either BOOTP or DHCP (described below) is required in a network-boot environment. BOOTP is not used in local-boot environments.

Note

Since DHCP has mostly superseded BOOTP, it is recommended that DHCP be used instead of BOOTP for network boot.

Note

BOOTP is not currently supported by Microsoft NT, although it is supported by Windows 2000.

When booting in a network environment, BOOTP provides the terminal with the following required information: the terminal's IP address; the IP address of the TFTP boot server; the pathname of the operating system file to be loaded using the TFTP server; the NFS directory to use for the terminal's root file system (including NFS server IP address and pathname on that server); and a subnet mask (typically 255.255.255.0 for Class C IP addresses and 255.255.0.0 for Class B IP addresses).

For network boot, the terminal should have the following pieces of information, but they are not necessarily required for the terminal to function (depending upon your network configuration). Recommended information includes a domain name, domain name server(s) to provide name-to-IP address resolution (for other terminals and/or computers), and gateway IP address (for allowing you to access computers outside your subnet).

Note

Some BOOTP server implementations allow only 64 bytes of information, including identification overhead, to be sent in a reply message. If the provided information plus overhead exceeds this limit, the server will truncate the reply message to fit within the limit, with unpredictable results. SCO Openserver contains a BOOTP server with this limitation. This has been reported to SCO and may be fixed in a release of Openserver after Release 5.0.5. Because of this restriction, the `T17` option (see below) may necessitate putting the terminal's root directory off the server's root directory (can be via a symbolic link).

To use BOOTP, you must typically make one entry per terminal, with an identifying tag and the terminal's MAC address. Of the fields mentioned above, the *only* field that *must* be unique for each terminal is the IP address field. Therefore, if using a BOOTP server that stores data in the `/etc/bootptab` file, the file can take a generic approach for all other fields and use the `tc` entry for each terminal to refer back to that generic entry, as in the following example:

Figure 2-1 Bootptab File Example

```
.c_terminal:ht=1:ds=132.237.1.42:gw=132.237.20.1:sm=255.255.255.0:\
    :dn=xx.com:sa=132.237.20.2:hd=/tftpboot:bf=vmlinux:\
    :T17="132.237.20.2:/nwt/root":
term1:ha=00800c123456:ip=132.237.20.5:tc=.c_terminal
term2:ha=00800c123457:ip=132.237.20.4:tc=.c_terminal
```

Legend:

bf	=	TFTP boot file
dn	=	domain name
ds	=	domain name servers (IP)
gw	=	gateways
ha	=	hardware address
hd	=	home directory
ht	=	hardware type
ip	=	host IP address
sa	=	TFTP server address
sm	=	subnet mask
tc	=	template host (points to similar host entry)
T17	=	root path

The option used here for the NFS root directory is the `T17` entry, which is of the form `IPADDR:/PATH`. The `IPADDR` entry is the IP address of the NFS server and `PATH` is the full pathname on that server to what will be the root directory of the network boot directory tree. (The quotation marks are required in the `T17` entry to allow the colon in the option data to be passed as part of the data.)

Note

IMPORTANT! The addresses of servers that support the terminal boot process must be specified by IP address. This is because the name resolution function is not operational until the system is completely loaded and initialized.

For all non-Windows server platforms, `bootp` can be run either at boot or from `inetd`. It is recommend that `bootp` be run from `inetd`, although with many terminals and a stable environment (i.e., an unchanging list of terminals), it may be faster to run via automatic start-up at server boot. Consult the manual pages for the `bootp` program on your server platform. Linux uses `bootpd`, UnixWare uses `in.bootpd`, Openserver uses `bootpd`, and HP/UX uses `bootpd`. On Linux and Openserver platforms, the entry to look for in the file `/etc/inetd.conf` (`/etc/inet/inetd.conf` on UnixWare) begins with `bootps`. On Linux, HP/UX, and Openserver platforms, the table that describes what options to provide to what terminals is `/etc/bootptab` (`/etc/inet/bootptab` on UnixWare). For more information, refer to the server manual pages that discuss `bootptab` and `bootpd`.

DHCP

DHCP is a protocol that can be used in both local- and network-boot environments. In local-boot environments, it can be used to reduce the amount of configuring that must be done on a terminal-by-terminal basis. In network boot environments, it can be used in the same manner as BOOTP (described above). For network boot, site policy should dictate the use of BOOTP or DHCP for providing the terminal with its boot information. In the database for DHCP, the terminal's MAC address and IP address are not normally used because all information typically will be provided for all terminals and the DHCP server manages the IP addresses for all terminals at run time.

Note

A Microsoft NT DHCP server can provide information allowing a terminal to network boot, provided the TFTP and NFS services are running on supported servers.

In a network-boot environment, all fields mentioned above for BOOTP should be entered and the same explanations apply. There are currently no other special requirements for configuring DHCP servers to provide information to the terminals. The server and path are provided to terminals by the DHCP protocol. DHCP uses options 66 and 67 defined in RFC 2132.

In a local-boot environment, DHCP can provide a set of configuration parameters, which reduces the need to configure the terminal's **Select | System | Setup | Connectivity | Internet | DHCP** dialog box. The default (out of the box) configuration assumes DHCP provides all network configuration information. As such, the fields mentioned above for BOOTP all apply, except that the TFTP server (`sa`), TFTP boot file (`bf`), and Root directory (`T17`) are not used. Providing them in a mixed (local- and network-boot) environment is acceptable, since they are ignored completely in a locally booted terminal.

Boot Server (see on-line help), otherwise known as "Buddy Boot," uses these options to give preference to a server that provides these options, servers for use with local boot should use these options with extreme caution, since it may prevent Boot Server from working.

The terminal renegotiates address information based upon the server's configured value for the lease time. If lease time is set for an infinite lease, the terminal will not renegotiate for a lease extension or a new IP address until the terminal is rebooted. At reboot, the terminal will once again ask for an IP address and other configuration information.

The terminal uses the DHCP options listed in Table 2-1. Future releases may increase the size of the list. Some of the listed options are sent by the server and others are sent by the client. Refer to the RFCs (listed in "*References"* in the "*Overview"* chapter of this document) for usage.

Table 2-1 DHCP Options

Option Number	Option Description
1	Subnet Mask
3	Router
6	Domain Name Server
12	Host Name
15	Domain Name
17	Root Path
18	Extension Path
28	Broadcast Address
43	Vendor-Specific Information
48	X-Windows Font Server
49	XDMCP Addresses
51	Lease Time
52	Option Overload
53	DHCP Message Type
54	DHCP Server IP Address
55	Parameter Request List
57	Maximum DHCP Message Size
58	T1 (renew) Time
59	T2 (rebind) Time
60	Vendor Class Identifier
61	Client Identifier
66	TFTP Server Name
67	Bootfile

Option 48 assumes TCP and port 7100 for font server access. If other ports are to be used, you must use the vendor-specific option described below. Also, option 49 assumes Query mode. If Direct is wanted, use the vendor-specific option.

The terminal uses options 66 and 67 to determine where to obtain the operating system for the network-booted terminal, with option 66 being the server name (as an IP address), and option 67 being the full pathname to the file (such as `/tftpboot/vmlinux)`. Option 17 is the IP address and path name to the root directory (similar to the `T17` entry for BOOTP) and is of the form `IPADDR:/pathname`.

Option 18 (extensions path) operates as follows: If the extensions path option is given, it is treated as a `<machine>+<directory-path>` pair, with a colon separating the two. Directory separators are UNIX separators. Typically, this would be of the form: `132.237.20.164:/tftpboot/extension.opt`, where the suffix is anything but `.txt` to behave consistent with RFC 2132. If the suffix is `.txt` (case is ignored), the file is treated as a text list of options in the form `option=value`.

Although this violates the RFC, text files are much easier to manipulate using an editor than is a DHCP option space. The IP address and pathname used above are only for example. Table 2-2 lists all T1500-specific options not listed in Table 2-1. Note that binary options can not be passed (as binary) in the text mode associated with this option.

If the DHCP server is capable of returning values for option 43 based upon either vendor or client ID (or some other tag), the current software release will utilize this data. The format of this option is an encapsulated format, consistent with RFC 2132. Identical options are available here, through the extensions path and through options 128+ (discussed below), although option 43 predefines the "option" numbers, while the others do not (unless option 43 is passed in the extensions path file).

Additional vendor-specific options are available to disable swapping and to provide a network services directory. These options are listed in Table 2-2 and sit in option space 128-254. Setup provides the ability to modify the set of options sent by the terminal to the server at DHCP negotiation time. By default, none of options 128-254 are requested. All vendor-specific options in the 128-254 option space are strings of the form `0080_TAG=DATA`, where `TAG` and `DATA` are illustrated in Table 2-2. It is recommended that, where possible, options 43 and 18 be used rather than the 128-254 option space.

Table 2-2 Additional Vendor-Specific Options

128-254 Tag	Option 43 Number	Description	Type/Length/Value for Option 43
	1	Vendor-specific ID.	Integer 4, 0x76583A1C
NETSVC	2	Network service machine and directory.	String, variable, same format as option 18 string.
NOSWAP	3	If this option is provided, swapping is turned off.	Integer 1, any value.
REFLASH	4	If this option is provided, the reflash utility is invoked in a network-boot environment.	Integer 1, any value.
MF_DIR	5	Server and directory where images reside for reflash utility.	String, variable, same format as option 18 string.
MF_CFG	6	Server and full pathname to configuration file for reflash utility.	String, variable, same format as option 18 string.
XFS	7	X font server list to include.	String, variable, same format as option 18 string.
XDMCP	8	XDMCP list.	String, variable, same format as option 18 string.
BUDDY_BOOT	9	If this option is provided, it indicates that we are providing the client with network-boot information for use with the Boot Server feature (also known as “Buddy Boot”).	Integer 1, any value.

Since an option can potentially be provided in three places (standard DHCP packet, option 43, and via TFTP with option 18), the precedence rule is defined as: (1) standard packet, (2) option 43, and (3) TFTP via option 18. Multiple instances of the same tag may occur in the system; only the first occurrence is used by the system. By precedence, we mean that data is read first by processing (1), when that is done, (2) is processed, followed by (3). Any option that is defined is not replaced by subsequent sections.

In a network-boot environment, the client and vendor identifiers are not modifiable by the user.

The terminal provides the ability to change the Client ID, Vendor ID, and Hostname fields consistent with the RFCs. The default Vendor ID is `Compaq-T1500`. The default client ID is the MAC address with a key (consistent with the RFC specifications). The default hostname is the letter “t” followed by the last 6 digits of the MAC address. Hostname is not exported by default, but the other two are.

Also, because of the need to guarantee compatibility with a Microsoft Windows NT/2000 environment, an option is provided (configurable in setup) to append a NULL character to the end of all string data, making it look like a Microsoft device (select **Select | System | Setup | Connectivity | Internet | DHCP | Advanced | Microsoft Server** check box). This option is not required, and should only be used if you can not do what you need to in your particular network environment. The software is normally able to work with Microsoft servers, although there may be some cases that require this option to be set.

Because of the established administration strategy, the default behavior is for the terminal to request NO options in the 128 through 254 “site-specific” option space. Because this is known to cause problems in some environments, Setup can be used to modify the set of options requested, after your administration strategy is in place. Any option used in this space is also available through option 18 or through option 43, if you choose to use those methods instead.

T1500-Specific Option Definitions

The T1500-specific options are defined in the following subparagraphs.

Option 43 Vendor-Specific ID

This integer field is a key that is used to indicate that the option 43 data is indeed intended for use with a T1500 terminal. If vendor-specific Option 1 is not provided, or if its length is not exactly 4, or if its value does not match the tag value listed in Table 2-2, the option 43 data is ignored in its entirety.

NETSVC

An additional set of software is provided to be stored on a server for use with the terminal. This image can be stored in either Windows environments or UNIX environments, and exported as a share or via NFS, as appropriate. This option provides the network path to this directory. The syntax for NFS is `machine:/path`, where `machine` is the IP address or DNS-resolvable machine name for the server, and `path` is the full pathname to the directory. The syntax for SMB (Windows server) is `//machine/share[/directory]`, where `machine` is a

DNS resolvable machine name, `share` is the share name, and `path` is an optional path within that share. For name resolution, an entry in the terminal's host file (**Setup | Connectivity | Internet | DNS | Hosts**) qualifies. For NFS, the directory MUST be exported with read/write/execute permissions and with root mapping to root, not to nobody. For SMB, the server's guest account needs to be activated and guest users need to be able to connect to that share for full control. The network services tree is automatically included as part of the network boot tree, so network services are not required here, but can be used to share the load between multiple servers. If large pages are to be printed, it is recommended that local-boot terminals use network services to provide space for the spool files.

NOSWAP

Normal behavior for the terminal is to allow swapping via NFS (network services or network boot), although not activating this ability. Setup provides the ability for a terminal to turn on swapping and specify the size of the swap file. Because of the server resources required to support swapping (20+ MB per terminal that can swap), the NOSWAP DHCP option allows the network administrator to override what is configured in setup, to protect the disk space capacity on his server. For Option 18 or 128+, this is a string `0080_NETSVC=YES`. For Option 43, it is a field with one byte of data. The data is ignored; however, including the option prevents swapping.

REFLASH

Normal behavior is to bring up the terminal's user interface in a network-boot environment. If this option is provided, the flash build utility is brought up and the terminal is put in a special mode, designed to reprogram itself or to program cards. Normally, this option is used only for the terminal’s Boot Server feature, which allows one terminal to be used to provide resources for other terminals to reflash themselves. For Option 18 or 128+, this is a string `0080_NETSVC=YES`. For Option 43, it is a field with one byte of data. The data is ignored; however, including the option prevents swapping.

MF_DIR

When using the flash build utility, this option provides the network services-style path to the directory where the images to be programmed reside when shortcuts are used by the flash build utility. The syntax for NFS is `machine:/path`, where `machine` is the IP address or DNS-resolvable machine name for the server, and `path` is the full pathname. The syntax for SMB (Windows server) is `//machine/share[/path]`, where `machine` is a DNS resolvable machine name, `share` is the share name, and `path` is an optional path within that share. For name

resolution, an entry in the terminal's host file (**Setup | Connectivity | Internet | DNS | Hosts**) qualifies. For NFS, the directory MUST be exported with read/write/execute permissions and with root mapping to root, not to nobody. For SMB, the server's guest account needs to be activated and guest users need to be able to connect to that share for full control.

MF_CFG

When using the flash build utility, this option provides the network services style path to the file that contains the list of images that are available for programming. The syntax for NFS is `machine:/path`, where `machine` is the IP address or DNS resolvable machine name for the server, and `path` is the full pathname. The syntax for SMB (Windows server) is `//machine/share[/path]`, where `machine` is a DNS resolvable machine name, `share` is the share name, and `path` is an optional path within that share. For name resolution, an entry in the terminal's host file (**Setup | Connectivity | Internet | DNS | Hosts**) qualifies. For NFS, the directory *must* be exported with read/write/execute permissions and with root mapping to root, not to nobody. For SMB, the server's guest account needs to be activated and guest users need to be able to connect to that share for full control.

XFS

DHCP provides a standard option for font servers. The standard option (48) is a list of IP addresses and assumes that the font server will be on port 7100. If you want to define your font servers by machine name rather than IP address, or want to run them at a different port (HP/UX puts its font servers at 7000 by default), you must use this option. The data is a comma-delimited list of font servers, of the form: `tcp/machine[:port]`, where the port is optional. The machine can have either an IP address or a DNS-resolvable name.

XDMCP

DHCP provides a standard option for XDMCP. The standard option (49) is a list of IP addresses that the terminal treats as XDMCP queries. If you wish either to provide XDMCP Indirect connections (where the other side of the connection provides a list of who you can connect to) or to provide a DNS-resolvable name, you can use the T1500-specific option.

BUDDY_BOOT

This flag is set by a DHCP/BOOTP server to distinguish a network boot from a Boot Server boot (otherwise known as “Buddy Boot”). A terminal that provides Boot Server service will set this; otherwise, this option should never be used.

Packet Size

The terminal is capable of sending and receiving the Maximum DHCP Message size option, allowing packets to contain up to 1500 bytes, including the DHCP header in this size. Since some DHCP servers will only respond to packets that are of the smallest size, the packets sent by the terminal are guaranteed to fit in a minimum size. If the DHCP server does not honor option 57, or honors one smaller than the one the terminal accepts, the terminal will operate successfully. Since the terminal always requests option 57 and always sends the minimal packet size, the terminal should not be limited in functionality in this manner.

The more options the server sends back to the terminal, the larger the packet must be. The DHCP protocol allows for this in guaranteeing that options are complete when they are sent and that options that will not fit in the remaining option space will not be sent. Which options are not sent are determined by the DHCP server.

In a heterogeneous environment, where DHCP is being used to configure multiple types of devices, it is recommended that the Client ID, Vendor ID, Hostname, or some other tag be used to define which set of option data is to go to which category of devices.

Some BOOTP servers limit the option space to a total of 64 bytes.

Option Overload

DHCP provides a mechanism for putting more option data in the DHCP packet in certain cases. The terminal is capable of using the Option Overload option to request that up to 192 extra bytes of the DHCP packet be available for use as option data. If the DHCP server is capable of filling in the SNAME and FILE fields in the DHCP header and responds to Option Overload correctly, the terminal is capable of using that data. It has been discovered that the current beta versions of the ISC DHCP server incorrectly responds to this option and produces corrupted packets if the data would overflow into this space (there is no problem if the data fits entirely within the normal option space). Currently no other DHCP servers have been found that support Option Overload.

Option 18 vs. Option 43 vs. Options 128+

All three methods (Option 18, Option 43, Option 128+) provide identical capabilities, just in different manners. It is recommended that only one method be used, but you are not restricted to this. Things to take into consideration when choosing include the following: existence of a TFTP server, level of configurability in the DHCP server, availability of a binary file editor, knowledge of DHCP option data format, and the number of other devices that are going to be administered via DHCP.

Option 18

Option 18 is a standard DHCP option that provides the network address and pathame of a file to be obtained via TFTP. The standard format of this file (RFC-defined) is a set of DHCP options (option number, length, data), terminated with the end (255) option. Since in most cases this format is very difficult to edit, a text file format is also supported where the options are of the form LABEL=DATA, all entries are one per line, and all are ASCII data. Any option that can be passed as DHCP option data can be stored in the binary format; only those which are actually supported by the terminal are allowed in text format. All 128+ options as described above are also allowed in an option 18 file.

Table 2-3 lists the labels and data for the text format options.

Table 2-3 Labels and Data for Text Format Option

Option Number	Label	Notes
1		Not allowed.
3	ROUTER	Put here with extreme caution.
4	TIMESERVER	Not currently used.
6		Not allowed.
9	LPRSERVER	Not currently used.
12	HOSTNAME	Put here with extreme caution.
15		Not allowed.
17		Not allowed.
18		Not allowed.
28		Not allowed.

Table 2-3 Labels and Data for Text Format Option, Continued

Option Number	Label	Notes
40	NISDOMAINNAME	Not currently used.
41	NISSERVER	Not currently used.
42	NTPSERVER	Not currently used.
43		Not allowed.
48	XFONTSERVER	First element; subsequent elements append a number contiguous to the label.
49	XDMCP	First element; subsequent elements append a number contiguous to the label.
51		Not allowed.
52		Not allowed.
53		Not allowed.
54	DHCPSERVER	Put here with extreme caution.
55		Not allowed.
57		Not allowed.
58		Not allowed.
59		Not allowed.
60		Not allowed.
61		Not allowed.
64	NISPLUSDOMAIN	Not currently used.
65	NISPLUSSERVER	Not currently used.
66		Not allowed.
67		Not allowed.
69	SMTPSERVER	Not currently used.
70	POP3SERVER	Not currently used.

Files ending in a `.txt` name are treated as text files. Any other filename is treated as an RFC-compliant file.

Use of this option requires a TFTP server. Since path names are included in the file, the TFTP server must accept UNIX-style file separators, not DOS-style separators. Likewise, the default transfer mode must be binary, and the file (either format) must be capable of being read by the terminal without modifications (i.e., the terminal does not accept carriage returns at the end of lines).

This provides the ability to give arbitrarily large option data to the terminal, bypassing the limitations of the Maximum DHCP Message Size option and some servers.

Option 43

Option 43 is the industry-standard method for providing vendor-specific option data to network devices. The three disadvantages are: the total length of option 43 (i.e. all vendor specific options) is 255 bytes; the option data is typically hard to enter; and some servers do not maintain different scopes of option data based upon Vendor ID, Client ID, or other device-defining tag. The Option Ids for these options are listed in an earlier table.

Options 128+

There is debate in the DHCP community about whether or not options 128 through 254 are for vendors' use. If your server is incapable of sending different option 43 values based upon an identifier, if you can not use TFTP, if you do not want to edit binary data, or if the total set of T1500 options is greater than 255 bytes, all T1500-specific options are available as text strings in this option space. All T1500 options have the prefix 0080_ and are described in an earlier table. By default (i.e., without configuring), the terminals request none of the 127 options in this space. By running **Setup**, the set can be increased. Any T1500 option can be placed anywhere in this option space, since the 0080_ tag is checked to determine whether or not it is a valid option. If you know what option numbers are going to be used, you can use **Setup** to define the requested set to just this set of option numbers; if you do not know, you can expose the entire option space.

TFTP

TFTP is required in a network-boot environment. The TFTP server loads the terminal's operating system off the server into memory on the terminal. This operating system then controls all other actions performed from the terminal. This resource is used once each time a network-boot terminal is powered-up. If a local-boot environment uses DHCP, and DHCP supplies option 18, the server named in option 18 must support TFTP. The load on the server is the amount of server resources required to copy approximately 1 MB of data from the server to the terminal, for each terminal being turned on. The address of this server (and the location of the file) is provided to the terminal, either by BOOTP or DHCP (see above).

TFTP can also be used in conjunction with DHCP for providing additional options to the terminal via DHCP option 18.

Note

TFTP is not supported for Microsoft NT.

For most UNIX systems, including Linux, SCO Openserver, and SCO UnixWare, TFTP is launched via the `inet` program. To activate TFTP in this way, there must be an entry in the `/etc/inetd.conf` (or `/etc/inet/inetd.conf`) file whose first column is `tftp`. Depending upon the platform, TFTP can be run in either a secure manner (every terminal connecting to the server via TFTP has access to only the directory specified in this file) or in an unsecure manner (access to the full system). Consult the documentation for the TFTP server (`in.tftpd` for Linux and UnixWare, `tftpd` for SCO Openserver) by running `man tftpd` on the platform in use by your organization.

NFS

NFS is a protocol that allows directories residing on one computer to be accessed from another computer or terminal.

Note

NFS is not yet supported for Microsoft NT.

This section describes the requirements for NFS configuration with respect to the directory tree that allows a network-boot terminal to have access to the same information as that for a local-boot terminal. (The information describing NFS configuration for the optional network services support is described in Chapter 3 of this document.)

The following four requirements are *mandatory* and ***must be met*** in the NFS configuration:

Note

IMPORTANT! If these requirements are not met, the terminals will not work in a network-boot environment.

1. The client root account map must be able to access the server root account (on Linux, this is called `no_root_squash`, and on SCO Openserver 5.05, set the NFS option to `-anon=0`). This is because the terminal executes certain software that (within the terminal environment) *must* be run as root, even when a user is logged in to the terminal. In UNIX, this is accomplished by making the programs set the superuser ID (`suid`) to root. If the NFS server remaps the ID to something other than root, the programs will run, but not as a root user.
2. The file system must support symbolic links.
3. The file system support must allow set-user ID programs to be stored (several Windows NT NFS implementations do not support this).
4. The file system must provide read/write access to the clients.

Note

The version of NFS provided with Red Hat Linux 5.2 has an inconsistency with versions in earlier releases. Normally, entries in the `/etc/exports` file should be of the form:

```
/nwt/root (no_root_squash)
```

For release Red Hat Linux 5.2, the default was changed from read/write to read-only, so the entry needs to be changed to:

```
/nwt/root\
(rw,no_root_sqash,no_all_squash)
```

for the system to behave correctly. Earlier and later versions of the NFS support will work properly with or without the explicit `rw` option.

DNS

DNS is a protocol designed for converting the relatively easy-to-remember descriptive machine/terminal names into IP addresses, which is their actual representation on the Internet/intranet. Although DNS is not required for the terminals to be functional, it is strongly recommended to use DNS. For example *www.name.com* is a lot easier to remember than a string of numbers (nnn*.n.nnn.nnn)*.

Many web sites have hard-coded names in their web pages, so if DNS is not configured, you will be able to get to the initial page but images and/or links on that page might not be resolved. Also, if DNS is not configured, you will need to configure every terminal's hosts database via the **Select | System | Setup | Connectivity | Internet** dialog box or use IP address notation for every user action that requires a computer name (such as e-mail addresses, POP3 server, Web access, etc.).

Time Server

Time Service supports the Internet Standard Time Protocol (see RFC 868). There are many locations on the Internet that provide time server information. If a time server is not available the user can set the time manually, but this will have to be performed every time the user logs in to the terminal. e-mail and some Web pages require the time, and time is displayed in the terminal's task bar; otherwise, time is not used by the terminal.

3 Configuring Optional Terminal Start-Up Resources

Several server resources can enhance terminal operation but are not among the minimum required for the terminal to function. The resources in this category use the following network protocols:

NFS	SMB	SNMP
HTTP	FTP	

and may use the following serial line protocols:

PPP	SLIP	CSLIP

This chapter provides a brief description of where the above-listed protocols are used and discusses any special configuration requirements. Some of the resources described here (such as NFS) have already been described in other chapters.

Network Services

Network services are software resources available on servers for terminals' use. Network services include:

- An additional set of software for use by diagnosticians in both network- and local-boot configurations.
- An additional set of fonts for use with the applications.
- The ability to load very large objects (e.g., from the Web) onto your terminal by making a swap area available on the network.
- The ability to print large objects by spooling them to a network file rather than keeping them in memory while printing and/or being sent to the printer server (or local printer).

Because of limited local storage capacity in the terminal, the fonts resident on the terminal are the minimum set for use with all applications. If a locally booted terminal uses the network services director, additional fonts are automatically made available. All the network services are already provided for the users who perform a network boot; no additional measures need to be taken to ensure that this group of users enjoys these benefits.

Note

SMB file sharing can not be used to support swapping; only NFS will support this function. All other services are supported by both file-sharing services.

NFS

Refer to Chapter 2 for more information on configuring NFS. The **Select | System | Setup | Administration | Network Services** dialog box can be used to configure the terminal for both swapping and print spooling.

In a network-boot environment, spooling is automatic and is on the root NFS directory tree as described in Chapter 2. Swapping is optional, with the size of the swap area based upon the setting of the slider in the **Network Services** dialog box. Swapping can be disabled through the use of DHCP options as described in Chapter 2.

In a local-boot environment, spooling is optional. If a network services directory is provided, spooling is available; otherwise, spooling is not available.

If NFS network services is desired, the information specified in Chapter 2 (with respect to permissions and mapping) applies. In addition, terminals write to the root directory of the NFS mount point, so permissions must be set accordingly.

SMB

SMB is the Microsoft network protocol used for file, directory, and print services.

If directory services are required, the network share, which is being exported as the network services directory, *must* be configured for guest access. It must not be password-protected for guest access, and must appear on a server browse list when queried from a remote computer. Ideally, the NT server that is providing the service will also be in DNS; otherwise, it must be put in the terminal's **HOSTS** file (under **Select | System | Setup | Internet | Hosts**) for name resolution to occur, and an IP address must also be associated with it. The terminal must additionally be able to create directories at the root level of the share and be able to create, modify, and delete files on the share.

For a network printer to be used (via SMB), all the requirements above must be met.

Also, for a server with an NTFS file system, the security must be altered to allow guests to have full access to all files and directories in the network services tree. Perform the following steps:

1. Use Windows NT Explorer to locate the folder in which network services is installed (`<drive>:\netservices` is the default).
2. Select **File** (or **Right**-click the mouse) to open the drop-down menu for the folder.
3. Select **Properties** to open the **Properties** dialog box for the folder.
4. Select the **Sharing** tab and select the **Shared As** radio button. Enter a share name (or use the default) and set the **User Limit** as desired.
5. Select **Security | Permissions | Add | Show Users**.
6. Select **Guest** and **Full Control**, then press **OK**.
7. Select both **Replace Permission** check boxes and press **OK**.
8. Reply **Yes** to the **Query** and press **OK**.
9. After the **Applying Security Information** process comp[letes, press **OK** to exit.

SNMP

SNMP is a network management protocol used for querying and modifying configuration information on existing terminals and other network devices. The terminal supports the standard MIB-2 associated with SNMP-v1, with the exception that most of the configuration information is read only.

For the current software release, the only fields that are modifiable are the read/write fields in the system group; specifically, the `system.sysContact`, `system.sysName`, and `system.sysLocation` objects. All other objects are currently read only. If your server is going to be used to configure and/or manage the terminals via SNMP, you should install the terminal MIB files, which are on the installation CD. Several standard MIBs are included on the CD and are named for the RFCs that describe them. These files do not need to be added to the network manager's database unless the NMS does not already contain a copy of the MIBs. Other than installing the SNMP manager software on your server and compiling the MIB into the manager's internal format, no additional configuration is necessary.

HTTP (Help)

HTTP is the protocol used by the World Wide Web. The server-based user help for the terminal is distributed as a tree of HTTP links and is on the installation CD. Terminal help can be installed on a WWW server, but because of network traffic or your configuration, it may be more desirable to configure a local HTTP server and install the help tree there. HTTP configuration is based upon the HTTP server software used, so refer to the installation documents that come with the HTTP software you are installing. There are no special requirements for using the help subsystem.

Serial Internet Connections

DNS routing has to be through either the terminal's serial port (**Select | System | Setup | Connectivity | Serial Internet**) or the Ethernet 10/100 Base-T connection (**Select | System | Setup | Connectivity | Internet**), not both. The resolver does not look up more than one domain. Linux requires that DNS be set up before working with SLIP/CSLIP or PPP. It will not accept the DNS information from the DNS server, so you must manually enter this in the DNS dialog section of the **Serial Internet** dialog box or **Internet** dialog box if you intend to use the PPP server's DNS.

PPP

PPP stands for Point-to-Point Protocol and is a standard serial line Internet protocol. Instructions for configuring the PPP server is best left to the documentation associated with the server, but the following restrictions apply to the client-side implementation for the terminal: Microsoft Windows NT RAS can be set up to use a variant of CHAP (Challenge/Handshake Authentication Protocol); the PPP connection will not work with this.

SLIP

SLIP stands for Serial Line Internet Protocol and is another standard serial line Internet protocol. It is does not provide error detection or retransmission services and does not compress data. Refer to the server documentation for configuration of the SLIP server. On the terminal, the host name and server name *must* correspond to entries in the host table.

CSLIP

CSLIP stands for Compressed Serial Line Internet Protocol and is a variant of SLIP that uses VJ header compression. The host and server name requirements mentioned under SLIP also apply to CSLIP.

FTP

FTP is one of the protocols that will be used to upgrade from the current software release to future releases. When implemented, configuration of an FTP server will be recommended, but the exact details currently are not available.

HTTP (Upgrades)

HTTP is one of the protocols that will be used to upgrade software to future releases. When implemented, configuration of an HTTP server will be recommended, but the exact details currently are not available.

4 Configuring Server Application Resources

Several server resources apply to the individual applications that run on the terminal. These resources are not needed for basic functioning of the terminal, but individual applications require them. The resources in this category use the following network protocols:

HTTP	POP3/IMAP4
ICA	RSH

This chapter provides a brief description of where each protocol is used and any special configuration requirements. Some resources covered here (such as HTTP) have already been described in previous chapters.

Refer to Chapter 5 for further information about browser resources.

HTTP

HTTP is the protocol used by the World Wide Web. If you are going to be using the browser to access pages within your intranet, you will need to configure your intranet web servers. HTTP configuration is based upon the HTTP server software used, so refer to the installation documents that come with the HTTP software you are installing.

If you are not using a browser and are not accessing any pages local to the intranet (including T1500 Help), you do not need to configure an HTTP server.

POP3/IMAP4

POP3 and IMAP4 are the Post Office Protocols used by the e-mail function embedded in Netscape Communicator on the terminal. If you are using the e-mail function to send and read e-mail, you may need to configure a POP3 or IMAP4 server to manage the e-mail. The e-mail user can also communicate with an individual's ISP account (if configured for POP3) to view that user's e-mail. Every user may need an individual account on the POP3/IMAP4 server. For instructions, refer to the server configuration documentation for the particular POP3/IMAP4 server being used.

Incoming e-mail is stored on the POP3 server until explicitly deleted. The system administrator may need to periodically remind users to delete unnecessary mail in order to reclaim space for normal operations.

ICA

ICA is the protocol used by the terminal to connect to servers running the Microsoft Windows Terminal (WTS) software and the Citrix Corporation MetaFrame software. ICA allows the terminals to run Windows applications remotely on the respective servers. If you are going to use the ICA client, you need to configure one or more servers running these services. To do this, refer to the documentation from Microsoft or Citrix. If you choose to use a remote browser via ICA, it too must be configured via the **Browser Location** dialog box (see Chapter 5 of this document).

RSH (X Manager)

RSH is a network protocol in a UNIX environment. It stands for Remote Shell. From the server side, RSH is typically accessed via an RSH daemon (such as `rshd` on Linux) that is enabled in `inetd.conf`. RSH provides the ability for one terminal or computer to execute programs that reside on another computer.

Note

Throughout this (RSH) section, references to `inetd.conf` refer to `/etc/inetd.conf` on Linux and Openserver, and to `/etc/inet/inetd.conf` on UnixWare.

Note

RSH support is not available from Windows NT servers. Even if X clients are installed on NT, RSH support must be available from other server(s) for the X Manager to be able to launch them.

The X Manager is the terminal's interface to RSH; on the server the following must typically must be configured for RSH support:

Note

For exact details refer to the manuals on your server.

First, `rshd` (or the equivalent) must be configured to respond to requests for application launching. Do this by modifying `inetd.conf` as appropriate for your system, or by running the appropriate system configuration tool.

Second, the server must be able to resolve a name from the IP address of the terminal. If the terminal IP address-to-name mapping is provided by DNS, nothing needs to be done. Otherwise, the server's `/etc/hosts` (or equivalent) file must be modified to contain the name that the terminal reports it has for that IP address. If DHCP services are used, but dynamic DNS (DDNS) is not in use, it may not be possible to construct a static table that correctly matches name and current IP addresses. If the terminal has a domain name, the name that matches the terminal's name will typically have the domain name as well.

Third, you must decide on how you are going to run the program. There are several approaches. There can be a one-to-one relationship for all terminal users to server users or there can be a many-to-one relationship for all terminal users to server users. The approach chosen will have many implications in the areas of security and privacy, and the choice should be made carefully. In the first case, you will need to provide accounts on the server for every terminal user. In the second case, you will need to provide a generic account on the server and have all X Manager sessions go through that account. For the one-to-one case, the entry in the X Manager **Edit Command** dialog box **Username** field should be `self`. For the many-to-one case, the entry should be the chosen account name.

After creating the account or accounts on the server, the `.rhosts` file in that account must contain the names of all users and terminals allowed to use that log in. The `.rhosts` file *must* be owned by the server user, and contains lines of the form

```
terminal<space>user
```

where `terminal` is the terminal name and `user` is the user name from the terminal (`root` is automatically used if security is disabled; `guest` is automatically used if security is enabled *and* `auto login as guest` is selected).

In addition, the terminal optionally supports both Kerberos authentication and DES data encryption for RSH commands, although the X protocol packets for an X application will not go through the DES data encryption layer.

Secure Shell

This is an additional method for using the X Manager with RSH. The distribution includes the shell `rshsecure`, which is designed to perform a more secure method for managing RSH requests. `rshsecure` also provides the ability for users to run shell scripts, such as those invoked from an XDM session on an X terminal. The remainder of this section describes how to configure your server for use with the `rshsecure` shell.

Start by creating a new account. For security reasons, make sure this account is *not* the superuser account.

As root, create a `.rhosts` file for this user, and make sure the ownership of the `.rhosts` file gets changed (`chown`) to this user. In the `.rhosts` file, add one entry for every terminal/user pair you want to go through `rshsecure`. For example, if you are using your terminals as “security disabled” and you are using DHCP, you can put every DHCP IP address in the `.rhosts` file with the user name being `root`. After saving the `.rhosts` file and using `chown` to assign ownership, make sure it is writable *only* by the user and not by anyone else (`chmod 644 .rhosts`).

Change the login shell for the account to be the `rshsecure` program (based upon where you installed it, since you need a full path name).

Note

On Linux, the included `rshsecure` binary uses `libc5`.

Determine the set of commands you will be allowing your users to run and create the file `rshsecure.cfg` in the login directory for this user. Again, make sure that it is not writable by anyone except the owner. Lines starting with the pound sign (#) are treated as comments. The first non-comment line is the shell to be used when invoking commands. The second non-comment line is the `xterm` program (or equivalent). The third non-comment line is the `su` program. All three of these programs should be fully qualified with path names to eliminate possible security concerns. All remaining lines are the authorized commands. The `rshsecure` program does a literal comparison of the entries in this file to the command passed via RSH (with arguments removed), so, for example, comparing `/bin/ls` to `/bin/ls` will succeed and comparing `ls` to `/bin/ls` will fail.

Any command executed through this mechanism will be run as that special user, although the SHELL environment variable is replaced with the first entry in the `rshsecure.cfg` file and the DISPLAY environment variable is set to point back to the terminal, allowing shell scripts that launch sets of X applications to work.

If the X manager specifies to run in this mode *and* provides an “actual user,” the `xterm` program (specified above) is executed, pointing back to the terminal, executing the `su` command (specified above). After the user successfully enters a password, the command passed via the X manager is then executed (SHELL and DISPLAY modified as above), with execution as this new user.

With the security and `su` capabilities described above, a `.xinitrc` file (or equivalent) can be executed, except that a window manager can not be launched (because the terminal is already running one). Every other application should run normally.

A prototype version of the `rshsecure.cfg` is provided on the CD and will be found in the same directory as the `rshsecure` program following installation.

5 Selecting Browser Location

The browser application is designed to run either locally or from a server. Normally it resides and is run locally. Based upon the number of users running an application, the processing power of the server, the types of operations being performed by the users with the application, and the type of network connection between the terminal and the server, it may be more advantageous to run the application from a server rather than locally. The application and reasons to choose local or remote operation are described in this chapter.

Browser Location

Your choice of browser location depends on both your browsing needs and the configuration of the terminal you are using.

The terminal uses Netscape Communicator. You may choose to execute Communicator locally or remotely. The selection is made using the **Select | System | Browser Location** dialog box.

Note

If you choose to run the browser remotely, it can be done via either ICA or RSH. Refer to the on-line help for instructions.

You may want to run the browser remotely for any of the following reasons:

- Heavy processing is better supported on a server.
- You have adequate network bandwidth at your location.
- Few users are on the network.
- You require specific plug-ins or mime types.
- You must save Web pages to a file.

- Your company has standardized on a browser other than Netscape Communicator.

Reasons to execute the browser locally:

- Less network bandwidth is available.
- You require faster start-up of the browser application.
- Many users are on the network.
- Your terminal is connected to the network via a serial or phone line.

If you choose to execute Communicator locally, there are several configuration options you may choose, each of which will enable different components of Communicator. Refer to the help available from within Communicator for instructions.

The user should also configure network services (**Select | System | Setup | Administration | Network Services**) for optimum performance of the local browser.

Because the network terminal has limited local memory, there are constraints on the use of Netscape Communicator. See the paragraph below for a summary of the constraints imposed.

Netscape Communicator Constraints

Netscape Communicator is made up of the composer, the navigator, and the mail/news subsystem. There is additional support for Java and Java applets. The following applies to Netscape 4.61, released in July 1999, running on the network terminal.

There are three boot models for the network terminal:

1. Network boot - in this environment, all the software is stored on a server and downloaded as necessary to the terminal client. Under this boot model, there is no issue with the Netscape Communicator on the terminal since nothing is stored locally.
2. Local Boot with network-based user directories - in this environment the user's home directory (other than root and guest) is stored on the network server. See the following table for constraints imposed to protect the flash memory.
3. Local Boot with local user accounts - this is the most precarious of environments. Anything saved is written to the flash file system. See the following table for constraints imposed to protect the flash memory.

Table 5-1 lists the various configurations of the terminal and the external controls that were imposed on Communicator for each configuration.

Table 5-1 Netscape Communicator Constraints

Configuration	Save/Save As	Java	Main/News	Composer
Local Boot:				
Local Home/No Swap	No	Yes	No	No
Swap	No	Yes	No	No
Net Home/No Swap	No	Yes	Yes	Yes
Swap	No	Yes	Yes	Yes
Network Boot:				
No Swap	Yes	Yes	Yes	Yes
Swap	Yes	Yes	Yes	Yes

Consequences:

1. In general, all cases of "Save," "Save As," and variants are hidden. This will only minimize the risk of the user encountering this operation. In the event one of these dialogs is displayed, the **OK** button is unavailable and the only recourse is to cancel out of the dialog.
2. The Composer is hidden.
3. Mail/News components are hidden.

6 Installing CD Software onto the Server(s)

This chapter describes the procedure for installing the software provided on the T1500 Windows-Based Terminal installation CD. The software is installed onto the server(s) you selected when filling out the worksheets for Chapter 1.

CD Contents

The CD contains a series of installation scripts, the programs necessary to run them on the supported platforms, the software (and other files) to be installed onto the appropriate server(s), the source code for components of the system that are protected by the GPL (GNU Public License), and the source code for the installation software.

Running the Installation Program

The installation script is designed to auto-configure itself for your platform and adapts to either a character or a graphical user interface. The only requirement is that you be the superuser (root) on UNIX or the Administrator on NT.

Note

You must be logged in as Administrator and not just a user with Administrator rights. On NT, the name used to log in must be administrator, and only the Server version of NT can be used to support the T1500 terminal

Caution

There is currently no check for sufficient disk space and no undo procedure. Total disk space required to install all software on the CD is 650 MB.

On UNIX, the script determines if GUI mode will be used based upon the DISPLAY environment variable; if it is set, the script uses the GUI, if it is not, it will run in text mode. This allows the installation to work graphically from a remote computer (such as installation from a UNIX workstation via Telnet to a server in a machine room), or non-graphically (running in the Telnet window). If you are operating remotely or as a superuser "`su`" logged-in to root from another user, make sure the access control has been disabled as required (using `xhost`).

Text and graphical installation modes both ask for exactly the same data. However, a Windows NT installation only prompts for information regarding supported features and prompts for less. Also, Windows NT only supports the graphical installation mode.

To determine the current user in a UNIX environment, the script looks at two environment variables. If USER is set, it is referenced for root/non-root permission. If USER is not set, LOGNAME is used in the same manner. This is because Openserver uses USER when logged in via X and LOGNAME when logged in through the text mode console.

After completing the worksheets (Appendix B) and determining the topology of your server environment, you will need to install the CD in the CD-ROM drive on your machine and mount the drive. For the same configuration as for the terminal test environments, the CD-ROM drive is as follows (by platform):

Platform	Drive
SCO UnixWare	`/dev/cdrom/c0b0t510`
SCO OpenServer	`/dev/cd0`
Slackware Linux	`/dev/cdrom`
Red Hat Linux	`/dev/cdrom`
HP/UX	`/dev/c1t2d0`

This may be different for your configuration. Consult your manual. For the purpose of describing the procedure, it is assumed the CD-ROM is mounted on a directory named `/cdrom`. Again, if you mount it somewhere else, make the appropriate interpretive changes as you go through this document.

Mount the CD-ROM drive using the following command:

Platform	Command
SCO UnixWare	`mount -r -F cdfs /dev/cdrom/c0b0t510/cdrom`
SCO OpenServer	`mount /dev/cd0/cdrom`
Slackware Linux	`mount /dev/cdrom/cdrom`
Red Hat Linux	`mount /mnt/cdrom /cdrom`

HP/UX	• To mount at the beginning:
	Make sure `/usr/sbin` is in the program search path.
	Do a `ps` to make sure the pfs software is not already running. If pfs is already running, skip the first 2 of the following commands:
	`nohup /usr/sbin/pfs_mountd &`
	`nohup /usr/sbin/pfsd -o bcbsize=4096 &`
	`pfs_mount /dev/c1t2d0 /SD_CDROM`
	• To unmount at the end:
	use `ps -ef | grep pfs` to find the `pfs` commands.
	You will eventually use `kill -9 <pidlist>` to kill the tasks, where `<pidlist>` is the list of process ID numbers returned by `ps` (the first column of numbers).
	To shut down the pfs software, change directory to / and unmount the device:
	`cd /`
	`pfs_umount /SD_CDROM`
	Perform the following two steps if the tasks were not running when the installation was begun:
	• Kill the rpc tasks (`pfs_mountd.rpc` and `pfsd.rpc`, in that order).
	• Kill the pfs tasks (`pfsd` and `pfs_mountd`, in that order).
	Make sure that you do this in the order specified or your server may crash. Make sure you leave the `pfs` software running for as short a time as possible, since HP indicates the machine may crash when this software is running.

Change the active directory to the CD-ROM drive (`cd /cdrom`).

Note

Windows uses " \ " as directory separator, and UNIX uses " / ". Prior to start of the TCL/TK runtime, use the appropriate separator.

Run the install procedure (`./install`). Note that `./install` explicitly runs the install program in the current directory. This is because there may be other install programs in your search path and because the current directory is not normally part of root's search path.

Answer all questions with the appropriate information (based upon your filled-out worksheet).

Note

Once in the installation scripts under Windows, the following file naming rules apply:

Use `c:/dir/file` as appropriate. You *must* use " / " instead of " \ ".

Do not use spaces in file or directory names.

You will be prompted as to whether this is an upgrade or an installation on top of a prior release.

- If you perform an upgrade, the configuration files from the prior release (assuming you pick the same directory for the upgrade) will be preserved rather than replaced. If you select upgrade of components not previously installed, they will be fully installed. There is no automatic uninstall of discontinued components.
- If you perform an installation on top of the prior release, the old configuration information will be lost. You will be prompted if attempting to overwrite directories.
- You may choose to selectively reinstall components of the current release, in which case only information pertaining to the reinstalled components will be overwritten. To ensure that the selected components are overwritten, select install rather than upgrade.

The installation script will not install any software onto your system until after all responses are entered. The last prompt will tell you when the installation is ready to proceed. Up until then, you can abort the installation safely by using the interrupt character (or by typing "q" for the yes/no prompts) for text mode or pressing the **Cancel** button for GUI mode. Text mode will abort immediately; GUI mode will ask for confirmation.

Although the procedures are similar for text and GUI modes, the following descriptions are provided individually for each mode since the user will only be installing in one mode on any one server.

By default, all installed software will be placed in a subdirectory of the /T1500 directory (which can be created beforehand as a symbolic link, if desired). The first location prompt will allow you to specify a new default. In picking the default, however, be aware that some BOOTP servers restrict you to a total of 64 bytes of options, so the root directory path must be short. If TFTP is configured on your server, the value given for its default will override your selected default for that one response, but you can change the directory, overriding the default (you will then need to fix the /etc/inetd.conf or equivalent file, as well). For Windows installation, the default is c:/T1500.

Note

If installing or upgrading and a prior release is on the system, it is recommended that you use the same servers and directories for the new release that were used for the old one.

Text-Mode Installation

The installation program output has been formatted for a screen of at least 24 lines by 80 columns. The installation consists of three types of operations:

1. You are asked which of the items on the CD you want installed on this server.
2. You are asked for file and/or directory names for the destination.

Note

Be careful not to overwrite installations for terminals using prior software releases

3. The files are installed in the appropriate places.

Directories are made as required, so a `/T1500/root` directory extraction will also create `/T1500`. If the directory and/or file exist at the time the second section of the installation is reached (querying for where to install), and if the user chooses to overwrite the data (applies to install only, not to update), the files and/or directories are removed prior to installing. This removes inappropriate files and directories (such as from an aborted installation). Upgrades will remove inappropriate (obsolete) files and directories as needed.

`Yes/No/Quit`-type questions have a `[ynq]` at the end of the message; there is no default response.

`File/directory`-type questions list the default in square brackets `[]`; there may be some with no default response. A leading slash is required for all files and directories.

If you desire to abort the installation, the INTERRUPT key will abort it before files are copied. Interrupting after the file copy operation has started will result in an incomplete installation. There is also a prompt after all the other prompts asking if you want to extract the data. A `yes` response will initiate the copy operation, and a '`no`' response will exit from the operation without updating your system.

GUI-Mode Installation

Upon execution of the install program, a background window is displayed which should cover the entire display. Window manager decorations (such as the title bar and buttons at the top of the window) will be displayed, but the program will ignore minimize, maximize, resize, and delete events. Under certain circumstances, some window managers will not always allow a child window to come up above the parent window (such as the default window manager on UnixWare). Where this flaw has been detected, the full-screen background window is not brought up.

Note

If the child window (the one with the text, check boxes, and buttons) is obscured, the key combination **Alt** + **Tab** can be used (multiple times if required) to bring it forward.

Note

If the child window (the one with the text, check boxes, and buttons) is obscured, the key combination **Alt** + **Tab** can be used (multiple times if required) to bring it forward.

There are five sections to the GUI-mode installation. Each has a distinct background screen. The first section is purely informative to you, the user. The second section contains a series of checklists, asking for which items you wish to install on that server. The third section asks for locations based upon the items selected in the second section. The fourth section confirms whether you wish to proceed and update your disk or abort your installation. The fifth section actually installs the software in the requested locations.

You will be presented with a series of dialogs. Most of the dialogs contain two buttons, **OK** and **Cancel**. **OK** will proceed to the next dialog. Except where noted, the **Cancel** buttons allow you to abort the current action.

Caution

Be careful not to overwrite installations for terminals using prior software releases. Do *not* select **Upgrade on top of a previous installation** when prompted.

Refer back to “Text Mode Installation” for additional information.

Installing on Non-Supported Servers

Although the installation software supports installation only on Windows NT server, SCO UnixWare, SCO OpenServer, Slackware, Red Hat Linux, and HP/UX servers, some end-users may want to use other servers. Patches to the CD software will be made available as new server platforms become supported. In the event that patches are not available at the time you require them, you can do one of two things: Either install the tar files (and other files) manually on your server or modify the installation script for use in your environment. Although the current software does not support either of these, the tools are provided so that you can do it if needed.

The entire installation procedure is written using TCL 8.0.3 and TK 8.0.3. TCL/TK is a scripting language similar to the shell and/or Perl, and is available for a large number of platforms (generic UNIX, Windows, Macintosh, and other systems). Tcl contains a non-graphical interface, TK adds a graphical interface.

The contents of the CD are separated into several directories. The `product` directory contains the terminal software. The `scripts` directory contains the TCL and TK scripts. The `sources` directory contains two `tar` files of sources, one for TK, one for TCL. The `library` directory contains runtime files that are common to all supported platforms but are not part of the actual installation scripts. The `images` directory contains the various background images for the installation screens (when run with a GUI). The `product.src` directory contains the source for the terminal components that are protected by the GPL (GNU Public License).

The upgrade directory contains the scripts necessary for upgrading local-boot terminals from one release to another.

The admin directory contains an ever-growing set of scripts that administrators can use or refer to for managing their terminals via NFS. The remaining directories contain the runtime environments for the various supported platforms, including TCL and TK binaries (tclsh and wish, respectively), shared libraries to guarantee a compatible environment (Linux), and other utilities that are used for the installation and are not normally part of the system being installed on (such as tar for NT). Any software that is not part of the standard release of the server OS will be installed as needed. At the ROOT directory of the CD, there are shell scripts for Windows (install.bat) and UNIX-like systems (install) that do minimal platform determination, set up the environment to run Tcl, and then change to the directory for the installation.

If you are going to rework the standard installation for your server, you will need to expand (“untar”) the two source files somewhere on your system, build them per the instructions in the tar file, and install them (per the instructions). You will need a C compiler to do this.

You first need to copy the CD contents to somewhere on your system. The following is a sample UNIX command:

```
mkdir /cdcopy; cd /cdrom; tar cvf - . | (cd /cdcopy; tar
xpvf - )
```

On most UNIX systems, this will copy the CD to the /cdcopy directory. Assuming you have a uname command, run it to determine the name of your system. Modify the install shell script (in /cdcopy) by adding an entry to the switch statement for your platform. Make a directory (off /cdcopy) for your server OS. Copy the TCL and TK binaries into that directory.

Now, go into the scripts directory (/cdcopy/scripts) and modify common.tcl (add a variable for your platform at the beginning variable block, add an entry to the switch for your platform), and fix the read_tftp_dir procedure.

If you are operating in a windowing environment and your window manager forces the installed windows to appear behind the background window, modify gui.tcl, and do the same operations as if $unixware != 0.

If your tar program performs in a non-standard manner, you will need to modify the full.tcl, help.tcl, netsvc.tcl, and nfsupgrade.tcl files accordingly.

A T1500 Windows-Based Terminal Quick-Start Instructions

The T1500 Windows-Based Terminal is shipped from the factory configured for local boot. Instructions are included in this appendix to convert to network boot if you require this mode of operation.

If you require additional network services for a local-boot (default) terminal, you must use the server setup procedure. This procedure starts with Chapter 1 of this document.

- OR -

If you change the terminal to boot from a network server, you must perform the complete server setup procedure that starts with Chapter 1 of this document.

Note

If the site has a DHCP server and the terminal connects through the network port, except for power and interface cable connections the administrator can perform all of the setup functions from a remote server. Refer to *T1500 Windows-Based Terminal Client Manager* on the *Software and Documentation* CD (requires Adobe Acrobat Reader). If the site has a DHCP server and the terminal connects through the network port, except for power and interface cable connections the administrator can perform all of the setup functions from a remote server. Refer to *T1500 Windows-Based Terminal Client Manager* on the *Software and Documentation* CD (requires Adobe Acrobat Reader).

Quick-Start Procedure

These instructions are for network administrators and end users already familiar with networks and terminals. They provide the minimum information needed to get the terminal into a basic operating mode that permits access to the full help system, services, and upgrade software residing on designated servers on the network.

1. Set the terminal on the desktop.
2. Connect the terminal communication interfaces.
   - A network-boot terminal must connect to the network through the network port; a network boot can not be performed through a serial port.
   - A local-boot terminal does not need a communication interface to boot. A communication interface is needed only to support the applications you are going to use.
3. Connect power (power module), VGA monitor, keyboard, and mouse.
4. Turn on power. After boot up completes, the desktop will be displayed and the **Select** button will appear at the left side of the task bar.
5. If this is a new terminal, upon start-up you automatically have administrator privileges and no password is required. Continue with the next step (step 6); however,
   - If the **Login** dialog box appears, log in using the administrator name “admin” or “root” and the administrator password. If you do not know the administrator password, try to log in with no password. If you can not log in as administrator, the terminal memory may need to be re-flashed.
   - If **Automatic Login as Guest** is selected from a previous session, the **Login** dialog box will not appear, and you will not be able to access the **Select | System | Setup | Administration** dialog boxes. In this case, use **Select | Setup | Files | Activate Logon** dialog box and enter a valid login name and password. Then select **Select | Shutdown** and **Login as a different user**, and log in as administrator.
6. If you want to change the terminal from local boot (default) to network boot, press the **Select** button at the lower-left corner of the desktop and select **System**. In the **Select | System** pop up menu, select **Setup**. This opens the **Setup** window, which has a menu bar from which dialog boxes may be opened. Click on **Administration** and select **Boot Model**. In the **Boot Model** dialog box select **Network Boot**. Click on the **Set** button, then re-boot the terminal (**Select | Shutdown**). The terminal is now set to boot from the network until the boot model is changed.

7. To further configure the network setup, use the **Select | System | Setup** window's **Connectivity** dialog boxes. Most of the information can be supplied by your network administrator:
   - For ethernet networking, make entries in the **Internet** dialog boxes.
   - For serial networking (network connection through a server), make entries in the **Serial Ports** and **Serial Internet** dialog boxes. Press the **Connect** button in the **Serial Internet** dialog box to make the connection.
8. To ensure access to the on-line help after access to the network is established, perform the following:
   a. Press the **Select** button at the lower-left corner of the desktop and select **System**. In the **Select | System** pop up menu, select **Browser Location**. In the **Browser Launch** dialog box, select **Local**, then select **Save**. (The local browser is the default and normally is already selected, but you should perform this step to be sure.)
   b. Press the **Select** button at the lower-left corner of the desktop again and select **System**. In the **Select | System** pop up menu, select **Setup**. This opens the **Setup** window. The **Setup** window has a menu bar from which dialog boxes may be opened.
   c. In the **Setup** window's **Administration|Network Services** dialog box, in the **Help** text box enter the IP address and path where the detailed on line help files reside. (The help files should be installed on a server by a network administrator. Refer to the server setup instructions starting in Chapter 1 of this document for instructions).

END OF QUICK START INSTRUCTIONS - Make any other desired selections in the remaining **Setup** window's dialog boxes. For more information, refer to the complete help instructions, which you should now be able to access via the network. It is suggested that before turning the terminal over to a user all **Connectivity** and **Administration** settings be made and the **Administrator and VNC passwords be changed from their defaults to assure security**.

"G-Key Reset" Procedure

You may reset the terminal software settings by using the G-Key Reset procedure:

- Turn on power and upon hearing the first beep *immediately* press the **G** key. The beep occurs coincident with expansion of the splash screen to full window size. The **Login** dialog box displays only if security is enabled, in which case enter a valid administrator or user login name and password.

  or

- If security is enabled, after turning on power you may wait until the **Login** dialog box displays. Press **Ctrl**+**G** and then enter a valid administrator or user login name and password.

  Follow the prompts displayed on the screen.

Note

Your security access level may limit the resets available to you. Refer to the on-line help documentation for details.

Note

If the screen display becomes disabled because a resolution or refresh rate incompatible with your monitor has been selected, power on the terminal and press the **S** key when you hear the beep. This will restore the display settings to 640x480 at 60 Hz (default), with which virtually all monitors can operate.

Note

If you converted the boot model to network boot and want to return to local boot, power on the terminal and press the **L** key when you hear the beep. This will permanently restore the boot model to local boot. To go back to network boot, repeat step 6 of the above procedure. The **G**-key reset does not reset the **L**-key action.

B Installation Planning Worksheets

The following worksheets should be filled in during the planning phase (Chapter 1) and used during the installation phase (Chapters 2 through 6) of your resource configuration process. The chapter corresponding to each worksheet provides specific information about the entries in the worksheet, and should be consulted as the worksheet is filled in.

Note

It is suggested that you make and use photocopies of the worksheets and retain the originals for possible later use.

The worksheets list the programs/components of the system required for each network resource. You do not have to use all the resources (e.g., if you are not going to use the network terminals to read or send e-mail (via Netscape), neither POP3 nor SMTP needs to be configured) and not all resources have to reside on the same server. Different resources that are used with the terminals can be distributed on different servers in a network environment, so that one (or more) servers can provide some services, and other servers can provide other services. In smaller installations, one server can be used to provide for all network services. In larger installations, the distribution of resources among servers can improve network performance, significantly in some cases.

Terminals are configured to boot locally as the default, but may boot from the network if desired (after power-on press **Ctrl** + **V** when you hear the beep, or use **Select | System | Setup | Administration | Boot Model for** a permanent change). Some resources are needed for network boot that are not required for local boot, and vice-versa. The worksheets apply to both boot modes of the terminal.

In an existing network environment where workstations are on people's desktops, many server resources may already be configured. In new installations you will have to determine which server resources you must configure for use with the network terminals, based upon your needs and environment (and filled in worksheets).

Terminal Start-Up Resources Worksheet

Installation Worksheet for Step 2 (Chapter 2)

Server Resource	Is software on the CD related to this resource?	Is the resource required for recommended for network boot?	Is this resource required or recommended for local boot?	Space required for CD components	Server Name (Write down the server name/IP address for each resource)
TFTP	Yes	Required	No	1M	
BOOTP	No	Required*	No	–	
DHCP	No	Required*	Recommended	–	
NFS (root)	Yes	Required	No	250 MB plus space for swap files and spooling on a per-user basis.	
DNS	No	Recommended	Recommended	–	
Time Server	No	Recommended	Recommended	–	

* Either BOOTP or DHCP is required, but not both.

Optional Terminal Start-up Resources Worksheet

Installation Worksheet for Step 3 (Chapter 3)

Server Resource	Is software on the CD related to this resource?	Is the resource required for recommended for network boot?	Is this resource required or recommended for local boot?	Space required for CD components	Server Name (Write down the server name/IP address for each resource)
NFS (network services)	Yes	Recommended	Recommended	200 MB plus space for swap files and spooling on a per-user basis.	
SNMP	Yes	No	No	1 MB	
HTTP (remote help)	Yes	Recommended	Recommended	40 MB	
PPP	No	No	No	–	
SLIP	No	No	No	–	
CSLIP	No	No	No	–	
FTP (upgrades)	No	No	No	–	
HTTP (upgrades)	No	No	No	–	
SMB (network services)	No	No	No	200 MB plus space for spooling.	
Admin Tool	Yes	No	Recommended	10 MB plus space for workspacaes.	

Server Application Resources Worksheet

Installation Worksheet for Step 4 (Chapter 4)

Server Resource	Is software on the CD related to this resource?	Server Name (Write down the server name/IP address for each resource)
HTTP (browser)	No	
POP3	No	
SMTP	No	
ICA	No	
RSH	Yes	

Browser Launch Location Resources Worksheet

Installation Worksheet for Step 5 (Chapter 5)

Server Resource	Is software on the CD related to this resource?	Server Name (Write down the server name/IP address for each resource)
ICA (remote browser)	No	
RSH (remote browser)	No	

Other Images Location Worksheet

Installation Worksheet for Step 6 Part 1 (Chapter 6)

Server Resource	Is software on the CD related to this resource?	Is the resource required for recommended for network boot?	Is this resource required or recommended for local boot?	Space required for CD components	Server Name (Write down the server name/IP address for each resource)
Repair Images	Yes	No	Recommended	60 MB	
Upgrade Images	Yes	Recommended	No	40 MB	
Upgrade Scripts	Yes	Recommended	No	10 MB	
Administrative Scripts	Yes	No	Recommended	1 MB	

Software Images from the CDROM Worksheet

Installation Worksheet for Step 6 Part 2 (Chapter 6)

Server Resource	Space required for CD components	Pathname recommendation*	Actual Pathname (Write down the pathname for each resource.)
TFTP	1 MB	`/tftpboot/vmlinux`	
NFS (root)	250 MB	`/mwt/root/`	
NFS or SMB (network services)	200 MB	`/mwt/netservices/`	
HTTP (help)	40 MB	`/mwt/help/`	
SNMP	1 MB	`/mwt/snmp/mib.txt`	
Repair Images	60 MB	`/mwt/local/`	
Upgrade Images)	32 MB	`/mwt/upgrade.fw/`	
Upgrade Scripts	1 MB	`/mwt/upgrade.sh/`	
Administrative Scripts	1 MB	`/mwt/admin.sh/`	
RSH Secure Shell	1 MB	`/mwt/rshsecure/`	
Admin Tool	10 MB	`/mwt/admin.tcl/`	

*Use “`c:/mwt/...`” for Windows NT Server.

T1500 Windows-Based Terminal Network Installation Guide

Created using FrameMaker® and Acrobat®

The on-line book is provided in PDF and presented on the terminal product CD.